IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*,

Defendants.

Hon. T. S. Ellis, III

Civil Action No.
15-cv-00662-TSE

PLAINTIFF'S REPLY BRIEF IN SUPPORT OF ITS MOTION TO COMPEL DISCOVERY RESPONSES AND DEPOSITION TESTIMONY

Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Road, #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

Benjamin H. Kleine (pro hac vice)
Devon Hanley Cook (pro hac vice)
Molly A. Smolen (pro hac vice)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

Ashley Gorski (pro hac vice)
Patrick Toomey (pro hac vice)
Jonathan Hafetz (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff

Table of Contents

Table of Authorities

Cases

Statutes

Other Sources

Rules

Introduction

Plaintiff Wikimedia has moved to compel responses to its discovery requests and deposition questions for the Court's in camera review pursuant to Section 1806(f) of FISA. These requests seek information that bears on whether some of Wikimedia's ubiquitous Internet communications are intercepted without a warrant as the NSA searches through Internet backbone traffic in conducting Upstream surveillance. Defendants, in opposition, have invoked the common-law state secrets privilege, arguing that Congress did not displace the privilege in FISA when it mandated that courts review surveillance-related information in camera.

Defendants' argument that Congress did not displace the state secrets privilege through FISA is untenable. In addition to overlooking the text and structure of the statute, that argument ignores Congress's overriding purpose in enacting FISA, which was to replace unilateral executive control over secret surveillance with a system of judicial review and accountability.

Because it is plain that Section 1806(f) displaces the state secrets privilege in favor of in camera judicial review wherever it applies, Defendants argue Wikimedia is not (yet) "aggrieved" under the statute—on the theory that Wikimedia has not yet proven it was surveilled. Defendants argue that a party is "aggrieved" under FISA only when the government has voluntarily revealed its surveillance. That interpretation conflicts with the text of the statute, and it would give the executive branch unilateral power to dictate who could challenge surveillance—a result at odds with the scheme Congress established in FISA to check executive branch surveillance.

Moreover, applying the in camera review procedure that Congress prescribed in FISA would not cause the harm that Defendants claim. First, the Court need not ever reveal the information it reviews in camera, whether at summary judgment or trial. Rather, it can simply rule that Wikimedia has or has not shown standing after reviewing the public record, which is

extensive, and the additional in camera materials. Because the Court will simply be assessing whether Wikimedia has shown a "substantial likelihood" of surveillance based on the totality of the evidence, its opinion need not reveal the specific contents of Defendants' answers. Second, even if the Court were to confirm that some of Wikimedia's ubiquitous Internet communications have been intercepted, that would not cause harm because it would not reveal new information about the scope of Upstream surveillance. Defendants have officially acknowledged their use of this surveillance to monitor Internet communications and "web activity" on a massive scale. The claim that adversaries would not already understand this Internet surveillance to encompass common web activities—like browsing Wikipedia—is not credible. Confirming that one or more of Wikimedia's trillions of Internet communications has been intercepted somewhere, at some point in the past ten years, would not cause "serious damage" to the United States.

Finally, in camera review is practicable, notwithstanding Defendants' exaggeration of the burden. As explained below, the Court will not have to review thousands of pages to determine whether Wikimedia has shown a substantial likelihood of surveillance.

I. In enacting FISA's in camera review provision, Congress displaced the state secrets privilege.

A. Congress established a comprehensive scheme to regulate foreign intelligence surveillance and thereby displaced the state secrets privilege.

As one pillar of the comprehensive legislative scheme it enacted in FISA, Congress expressly authorized civil actions challenging the lawfulness of electronic surveillance. *See* 50 U.S.C. § 1810. In Section 1806(f), Congress provided a mechanism that allows challenges to FISA surveillance to go forward while protecting sensitive information. Rather than exclude surveillance-related evidence as Defendants seek to do here, Congress displaced the state secrets privilege and directed courts to examine the evidence in camera as part of a regime that ensures independent judicial review of the executive branch's surveillance activities.

Nonetheless, Defendants argue that Congress did not speak clearly, unequivocally, or directly enough in FISA to displace the state secrets privilege. *See* Def. Opp. 24–25. Defendants claim that the statute is not clear enough to ever overcome the executive branch's invocation of the state secrets privilege to withhold evidence. *See id.* at 24, 28. That cannot possibly be correct.

As a threshold matter, the government is wrong in implying that the state secrets privilege is constitutionally compelled. While it may perform a function of "constitutional significance," *see id.* at 24, so too does Section 1806(f) in protecting the government's secrets against unwarranted disclosure. In any event, Defendants misstate what was required of Congress to displace the state secrets privilege in favor of in camera review. Defendants argue that a "clear and unequivocal statement" standard applies, and appear to suggest that Congress could "displace the state secrets privilege" only by using those exact words. *See id.* at 26.

But that requirement is not supported by Defendants' cases, and the same argument has been rejected by another court. *See In re NSA Telecomm. Records Litig.*, 564 F. Supp. 2d 1109, 1122–24 (N.D. Cal. 2008). Defendants rely on *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991), and *United States. v. Bass*, 404 U.S. 336, 349–50 (1971). Def. Opp. 24. However, in those cases, the courts confronted a legislative record that was silent, "scanty," or "meager" as to whether Congress had any intention of adjusting the balance of power as between the federal branches or as between the federal government and the states. *See, e.g.*, *Franklin*, 505 U.S. at 800; *Bass*, 404 U.S. at 345, 350. These courts did not announce a heightened standard that would apply here, let alone one that would nullify the in camera review procedure Congress expressly enacted. Rather, the courts reasoned, in the face of legislative silence or near-silence, that if Congress had intended to bring the President within the Administrative Procedure Act or to "change[] the federal-state balance"

in the criminal arena, Congress would have spoken more "clearly." *Bass*, 404 U.S. at 349.

There is no such silence here. In the text of Section 1806(f), in FISA's structure, and in its legislative history, Congress demonstrated its clear and unambiguous intent to regulate discovery of FISA-related information and to displace the state secrets privilege—imposing a comprehensive statutory scheme designed to constrain executive branch surveillance. *See* Pl. Br. 13–16.[1] Thus, regardless of the applicable standard, Section 1806(f) displaces the privilege.

First, Section 1806(f) speaks directly, clearly, and unequivocally to the question of what procedures apply "whenever" an aggrieved person seeks to "discover" FISA-related evidence. FISA mandates in camera review, and thereby forecloses the assertion of an absolute executive branch privilege. Section 1806(f), like the state secrets privilege, dictates how courts should address evidence where disclosure could threaten national security, and prescribes a process for the executive branch to assert such claims. *Compare* 50 U.S.C. § 1806(f) (requiring "an affidavit under oath that disclosure . . . would harm the national security"), *with United States v. Reynolds*, 345 U.S. 1, 7–8, 10 (1953) (requiring a "formal claim of privilege" demonstrating danger to national security). Because Section 1806(f) speaks to the same circumstances and controls "notwithstanding any other law," it displaces the privilege. *Id.*

Second, the structure and legislative history of FISA make clear that Congress intended to displace the state secrets privilege in civil cases like this one. Defendants ignore the full reach of the statute, which established both substantive and procedural remedies for surveillance abuses—including through civil litigation. After uncovering a long history of such abuses, the

[1] Defendants also suggest that Congress has not spoken clearly enough because any displacement of the state secrets privilege would represent a waiver of sovereign immunity. Def. Opp. 25 (citing *United States v. Reynolds*, 345 U.S. 1, 6 (1953)). But, unlike in *Reynolds*, Congress has expressly and unequivocally consented to the evidentiary rules that displace the privilege in cases involving FISA. That consent is contained in Section 1806(f) itself.

Church Committee called for the creation of civil remedies for unlawful surveillance, explaining that "courts will be able to fashion discovery procedures, including inspections of material in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Book II, S. Rep. No. 94-755, at 337 (1976). Congress implemented the Church Committee's recommendations by authorizing individuals to bring claims for unlawful surveillance. 50 U.S.C. § 1810. And, in enacting Section 1806(f), Congress expressly acknowledged that FISA's in camera review procedures would apply in civil cases. *See* H.R. Rep. No. 95-1720 at 31–32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060–61 ("an in camera and ex parte proceeding is appropriate . . . in both criminal and civil cases").[2]

Defendants cannot explain away the applicability of Section 1806(f) to civil cases, so they simply ignore it. But FISA's text, structure, and purpose confirm that Section 1806(f) is not limited to the two narrow scenarios Defendants claim: where the government provides notice that it intends to use FISA-based evidence, or where an aggrieved person moves to suppress evidence obtained or derived from FISA surveillance. Def. Opp. 20. By its plain terms, Section 1806(f) additionally applies "whenever *any motion or request* is made by an aggrieved person pursuant to any other statute or rule of the United States or any State *before any court or other authority* . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . ." 50 U.S.C. § 1806(f) (emphasis added). This catch-all provision encompasses

[2] The House of Representatives originally proposed two separate procedures, one for criminal cases and one for civil cases. H.R. Conf. Rep. No. 95-1720 at 31–32. In Section 1806(f), Congress ultimately adopted a single in camera review procedure for courts to apply in both criminal and civil cases. *See id.*

civil cases challenging the lawfulness of FISA surveillance.

The breadth of Section 1806(f) also reflects two critical facts about how Congress chose to ensure accountability through FISA. First, it reflects Congress's intent to channel *all* FISA-related discovery motions through Section 1806(f)'s in camera review procedures. Section 1806(f) represents Congress's decision about how to afford meaningful redress to individuals while accommodating executive branch claims of secrecy. Congress forbade parties from upending its decision by resort to other discovery rules. *See* S. Rep. No. 95-604, pt.1, at 57 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904. Here, Defendants play the "inventive litigant" by trying to thwart the application of Congress's chosen procedures. *Id.* Second, the breadth of Section 1806(f) is consistent with Congress's scheme to ensure judicial review of surveillance activities. If parties could rely on Section 1806(f) only in those instances where the government had chosen to acknowledge its surveillance, the civil remedies that Congress enacted would be illusory. The government could evade review of well-founded claims, as it seeks to do here, simply by invoking the state secrets privilege. That is directly at odds with the overriding purpose of FISA. S. Rep. No. 95-604, pt. 1, at 8; *In re NSA Telecomm. Records Litig.*, 564 F. Supp. 2d at 1122–24 ("Congress intended for the executive branch to relinquish its near-total control over whether the fact of unlawful surveillance could be protected as a secret.").

Defendants do not contest that Congress could constitutionally displace the state secrets privilege if it chose. The evidence is overwhelming that Congress did precisely that when it mandated in camera review of surveillance-related information.

B. Wikimedia satisfies the requirements for in camera review under Section 1806(f).

Wikimedia is an "aggrieved person" under FISA, and it is seeking a determination that Upstream surveillance of its communications is not "lawfully authorized and conducted." 50

U.S.C. § 1806(f). Defendants are wrong in contending otherwise. *See* Def. Opp. 21–23.

1. Wikimedia is an "aggrieved person."

FISA defines an "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). As the Fourth Circuit held, Wikimedia has plausibly alleged that its communications are subject to Upstream surveillance. *Wikimedia Found. v. NSA*, 857 F.3d 193, 210–11 (4th Cir. 2017). These allegations are more than sufficient to establish that Wikimedia is an "aggrieved person" as FISA defines that term.

The government argues it alone bestows "aggrieved person" status by confirming its surveillance. Def. Opp. 21. This is incorrect. Status as an "aggrieved person" is not predicated on the executive branch's say-so.

First, in *In re NSA Telecommunications Records Litigation*, 595 F. Supp. 2d 1077, 1083 (N.D. Cal. 2009), the court rejected the argument that "only affirmative confirmation by the government or equally probative evidence will meet the 'aggrieved person' test." It held that plaintiffs had "alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA's section 1806(f). . . . [T]o find plaintiffs' showing inadequate would effectively render [that] provision of FISA without effect." *Id.* at 1086; *see also* Hr'g Tr. 32:23–32:25, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. May 19, 2017) (ECF No. 362) (ordering in camera review under Section 1806(f) of evidence relevant to plaintiffs' standing where the government has not confirmed its surveillance). This approach comports with the text and structure of the statute, as well as common sense. Section 1806(f) cannot reasonably require the government's acknowledgment of surveillance—or a separate trial on whether a litigant is

aggrieved—before a party can access Section 1806(f)'s discovery scheme.[3]

Second, the definition of "aggrieved person" in Section 1801(k) is not limited to those the government acknowledges it surveils. As evidenced by FISA's notice provisions, 50 U.S.C. § 1806(c) and (d), Congress knew how to require notice. If Congress had intended to limit "aggrieved person(s)" to those who had received notice of surveillance, it would have said so.

Third, Sections 1806(c) and (d) contemplate that a person will be "aggrieved" *before* the government notifies him that he has been surveilled. *See id.* In other words, being an aggrieved person is a precondition to notice, not vice versa.

Fourth, Section 1806(f) commands in camera review in circumstances other than those involving government notice of surveillance. It states that when the government has provided notice under Section 1806(c) or (d), when a litigant moves to suppress evidence (regardless of notice), "*or* whenever any motion or request is made by an aggrieved person" to discover material related to the surveillance, the court must review the material in camera. The use of the disjunctive "or" makes clear that Section 1806(f)'s in camera review procedures apply in civil cases even absent notice to an aggrieved person.[4]

---

[3] The cases cited by Defendants are not to the contrary, as they do not address whether government notice is a prerequisite to aggrieved-person status, or whether a litigant can establish this status through plausible allegations, rather than by concession. *See* Def. Opp. 22–23. In particular, Defendants' reliance on *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991), is misplaced. In dicta, the court stated that a district court should assess the legality of challenged surveillance before disclosing materials *to a plaintiff*. *Id.* at 469. In contrast, here, Wikimedia seeks in camera review as prescribed by the statute.

[4] Although Defendants urge the Court to apply the interpretive canons of *noscitur a sociis* and *ejusdem generis*, these canons are irrelevant to the meaning of Section 1806(f). When interpreting statutes, courts rely on *ejusdem generis* only "to ensure that a general word will not render specific words meaningless," *CSX Transp., Inc. v. Alabama Dep't of Revenue*, 562 U.S. 277, 295 (2011), and on *noscitur a sociis* "to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words," *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995). Defendants point to no text in Section 1806(f) that even arguably renders other parts of the subsection "meaningless" or "inconsistent."

Finally, by authorizing in camera review for "any motion or request," 50 U.S.C. § 1806(f), Congress gave teeth to FISA's civil liability provision, *id.* § 1810. If access to in camera review under Section 1806(f) were contingent on government notice, the executive branch would have unilateral control over who could pursue remedies against it. That would undermine the very purpose of FISA and the balance Congress struck to address executive branch surveillance abuses.[5]

2. The information at issue will aid the Court's determination of whether the surveillance of Wikimedia is "lawfully authorized and conducted."

Defendants contend that the Court cannot rely on in camera review to determine whether, for the purposes of standing, Wikimedia's communications have been subject to Upstream surveillance. Def. Opp. 21. Not so. Section 1806(f) provides that, where the statutory criteria are satisfied, a district court "shall" review in camera materials relating to the surveillance "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). That is the question presented here.

As a general matter, adjudication of standing is part and parcel of any adjudication of the lawfulness of surveillance. This Court's analysis of standing is simply the first step in "determin[ing] whether the surveillance of [Wikimedia] was lawfully authorized and conducted." *Id.* In addition, as the Court has recognized, the standing and merits questions here are intertwined: the question of whether Wikimedia's communications have been subject to Upstream surveillance goes both to standing and to the merits of Wikimedia's claims. *See* Sept.

[5] Defendants cite legislative history that, in fact, supports Wikimedia's position. They argue that H.R. Rep. No. 95-1283, at 90 (1978), indicates that Section 1806(f) "sets out special judicial procedures to be followed *when the Government concedes that it intends to use or has used evidence obtained or derived from electronic surveillance*." *See* Def. Opp. 22 n.13 (emphasis by the government). But that House Report concerned an earlier version of the bill; the quoted language describes text Congress decided *not* to enact. *Compare* H.R. Rep. No. 95-1283, at 10, *with* 50 U.S.C. § 1806(f).

22, 2017 Hr'g Tr. 11–12, 31–33, 37–38, 43 (Def. Opp., Ex. A). The Court's in camera review would help it ascertain whether Wikimedia was subject to Upstream surveillance and whether that surveillance was lawful, just as Section 1806(f) contemplates.

Moreover, case law supports the use of Section 1806(f)'s procedures for the purposes of assessing standing. In *Jewel v. NSA*, the district court ordered the government to produce—for in camera review under Section 1806(f)—extensive evidence related to the plaintiffs' standing to pursue claims concerning electronic surveillance. *See* Hr'g Tr. 7:25–8:3, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. May 19, 2017) (ECF No. 362) ("Defendants shall be required to marshal the evidence to submit for an in camera review."); *id.* at 44:17–21 ("I want all of the documents . . . that bear on the issue of statutory standing"); *id.* at 51:23 ("When I say 'all,' I mean all."); Min. Order, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. May 19, 2017) (ECF No. 356).

Here, the Fourth Circuit has already held that Wikimedia's standing is plausible. At this point, after three years of litigation, the government cannot reasonably argue that the case has not come far enough for in camera review. That the government sought to artificially bifurcate these proceedings, as a matter of judicial economy, provides no basis for it now to argue that Section 1806(f)'s procedures are legally unavailable. Because Wikimedia is an aggrieved person, and because it seeks this Court's in camera review to determine whether FISA surveillance was lawful, Section 1806(f)'s procedures apply here.

C. *Amnesty International* is no bar to the application of Section 1806(f).

Defendants contend that if the Court were to conduct an in camera review, it would "inevitably lead to the disclosure of whether Plaintiff was subject to surveillance or not," and that such disclosure is prohibited under *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). Def. Opp. 31. Defendants are mistaken on both points.

In *Amnesty*, Justice Breyer proposed at oral argument that the government could resolve

the question of standing by disclosing to a court whether it was intercepting the plaintiffs' communications. 568 U.S. at 412 n.4. Notably, the plaintiffs had not served any discovery requests, and Section 1806(f) was not at issue. The Court declined to create a "disclosure proceeding" out of whole cloth, observing that the "hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program." *Id.* However, the concerns articulated in *Amnesty* are no bar to the application of Section 1806(f) here.

This Court could rule on Wikimedia's standing without disclosing *any* of the information it has reviewed in camera. In contrast to the proceeding described in *Amnesty*, neither Wikimedia nor the public would know precisely what evidence the Court reviewed in camera, because neither knows precisely what responsive information Defendants possess. In light of this ambiguity—as well as the substantial volume of publicly available information that will be introduced as evidence—the Court could craft an opinion without revealing the sources of evidence upon which it relied, and without revealing whether the government had confirmed that Wikimedia was in fact subject to Upstream surveillance.

The standard governing the standing inquiry reinforces this conclusion. Because Wikimedia seeks prospective relief, the Court need only address whether Wikimedia has established, by a preponderance of the evidence, that there is a "substantial risk" that its communications will be subject to Upstream surveillance. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Amnesty Int'l USA*, 568 U.S. at 414 n.5). The Court need not disclose whether the government has confirmed that Wikimedia was subject to Upstream surveillance in the past or that Wikimedia will definitely be subject to Upstream surveillance in the future.

In *Amnesty*, the Supreme Court declined to create a novel disclosure proceeding. But Section 1806(f) is not novel, and the Court's footnote of dictum does not control here. The concern articulated in *Amnesty* is simply not implicated by the facts of this case, where Wikimedia—with more than a trillion Internet communications each year and users in virtually every country on Earth, and whose standing was deemed plausible by the Fourth Circuit—seeks to use Section 1806(f)'s established discovery mechanism.[6]

Moreover, even if the Court were to confirm that one of Wikimedia's communications has been reviewed in the course of Upstream surveillance, it would not result in the risks to national security asserted by Defendants or hypothesized in *Amnesty*. *See* Def. Opp. 31–32; Pl. Br. 21. No target, terrorist, or spy would learn that his or her communications were (or were not) being surveilled. As the Fourth Circuit recognized, Wikimedia is no ordinary plaintiff. It is differently situated from the plaintiffs in *Amnesty* not only based on the volume and distribution of its communications, but because so much information about Upstream surveillance has been officially disclosed since those plaintiffs brought suit. *See Wikimedia Found.*, 857 F.3d at 211–12, 217. Because Wikimedia communicates with hundreds of millions of individuals scattered around the world, and because Internet communications take ever-shifting paths, disclosure that the NSA has reviewed one of Wikimedia's communications would reveal no new information about the scope of that surveillance. *See* Pl. Br. 21. Nor would disclosure "compromise" any collection capability related to Wikimedia or its users, as DNI Coats suggests, Coats Decl. ¶ 24

[6] Just as the Court could rule on standing without disclosing whether Wikimedia was subject to surveillance, it could rule on standing without disclosing whether Wikimedia is "on the list of surveillance targets," *Amnesty Int'l USA*, 568 U.S. at 414 n.5, or revealing the identity of any particular target with or about whom Wikimedia may have communicated. This is especially true in light of the fact that the government copies and reviews far more communications under Upstream surveillance than the millions it ultimately identifies as belonging to its targets. *See, e.g.*, PCLOB Report 111 n.476 (Upstream surveillance requires "access to a larger body of international communications" than those containing a targeted selector).

(ECF No. 138-2). Given the government's disclosure that it is monitoring Internet backbone traffic, including web activity, Wikimedia and its users already understand that at least some of their communications are subject to Upstream surveillance. Am. Compl. ¶¶ 57–67, 103, 107–111 (ECF No. 72). And theoretically, if the Court were to disclose that Wikimedia has *not* been subject to Upstream surveillance, it would not signal "that a particular individual has avoided scrutiny and is a secure source for communicating," Coats Decl. ¶ 23, because it would disclose nothing about whether the NSA had sought to target any particular individual under Section 702, nor would it provide any assurance against the interception of Wikimedia communications in the future.

The government's response to Plaintiff's analogy involving taxi cabs on the streets of New York—*i.e.*, Wikimedia's communications on the Internet—only illustrates this point. *See* Def. Opp. 11–12 n.6. Even if the NSA is a kind of undercover officer, it has already acknowledged its presence on the Internet, where it searches for communications associated with its targets. Indeed, it has already acknowledged monitoring "web activity," *see* June 1, 2011 FISC Submission at 30 (Toomey Decl., Ex. 25, ECF No. 125-28), and Wikimedia operates one of the top-ten websites on the World Wide Web. A finding that that one of Wikimedia's trillions of communications has been or is substantially likely to be copied and reviewed in the course of Upstream surveillance would not provide targets or adversaries with any new information.

D. Even if the state secrets privilege were available, it would not bar disclosure of all the evidence Wikimedia seeks.

Disclosure of much of the information Wikimedia seeks would cause no harm. For instance, it is not credible to suggest that disclosure of whether the NSA has reviewed one communication sent by one of the most popular websites on the Internet would endanger national security. *See* Barnes Decl. ¶¶ 57–58 (ECF No. 141-1). Though courts give deference to the

government's determination that disclosure of particular information would threaten national security, that deference is not a blank check. The Fourth Circuit has emphasized that "it is essential that the courts continue critically to examine instances of [the state secrets privilege's] invocation." *Abilt v. CIA*, 848 F.3d 305, 312 (4th Cir. 2017). Courts must review the government's claims "with a very careful, indeed a skeptical, eye," so as "not to accept at face value the government's claim or justification of privilege." *Id.* They must analyze whether, in fact, there is "a reasonable danger" that disclosure would harm national security. *Reynolds*, 345 U.S. at 10.[7]

The government has broadly invoked the state secrets privilege to withhold an array of other information responsive to Wikimedia's requests. *See generally* Coats Decl.; Barnes Decl. But for many requests, the government's explanation of the harm that would result from disclosure ignores the publicly available evidence. For instance, the government has refused to admit or deny that it conducts Upstream surveillance at "multiple" circuits or "multiple" chokepoints. *See* RFA Nos. 13, 15 (Toomey Decl., Ex. 1, ECF No. 125-4). However, as Wikimedia has explained, the PCLOB acknowledged that Upstream surveillance takes place on "circuits" (plural) with the compelled assistance of telecommunications "providers" (plural). *See* Pl. Br. 22 (citing PCLOB Report 35–36). In light of these acknowledgments, disclosing that Upstream surveillance takes place on "multiple" circuits would not "assist foreign adversaries" in evading monitored channels or exploiting unmonitored ones because it would disclose no new

[7] The government contends, without support, that "litigants seeking to compel disclosure of national security information on the basis that it already lies in the public domain must show that the information has been 'officially acknowledged.'" Def. Opp. 12–13. But the "official acknowledgment" test governs litigation over withholdings under FOIA, not civil discovery. Here, the question is not whether information has been "officially acknowledged," but whether disclosure would harm national security. *See Reynolds*, 345 U.S. at 10.

information. Coats Decl. ¶ 31.[8]

The government has also refused to admit that the NSA screened or screens the content of Internet web traffic. *See* RFA Nos. 37, 38 (Toomey Decl., Ex. 1). DNI Coats asserts that disclosing this information would "help[] our adversaries evade detection, which would seriously compromise, if not destroy, important and vital ongoing intelligence operations." Coats Decl. ¶ 27. However, the government has acknowledged Upstream collection of "web activity," *see* June 1, 2011 FISC Submission at 30, and it has acknowledged screening the contents of communications to identify those it seeks to retain, *see* PCLOB Report 36–37; NSA Dep. Tr. 261:8–10, 263:2–18 (Gorski Decl., Ex. 2). Accordingly, disclosure of responsive information could not harm national security, let alone destroy ongoing intelligence operations. *See also* Pl. Br. 22–23 (discussing other requests for which no harm would result from disclosure).

E. Sections 3024(i) and 3605(a) do not bar discovery in this case.

The government contends the information Wikimedia seeks is protected under 50 U.S.C. § 3024(i), a provision of the National Security Act instructing the DNI to "protect intelligence sources and methods from unauthorized disclosure." Def. Opp. 14–16. As explained in Plaintiff's opening brief, Section 3024(i) does not establish a litigation privilege. *See* Pl. Br. 23–24. But even if it did, FISA's more specific discovery provision, 50 U.S.C. § 1806(f), would control. *See, e.g.*, *Green v. Bock Laundry Mach. Co.*, 490 U.S. 504, 524–26 (1989). Notably, none of the cases cited by the government in support of its argument about the applicability of Section 3024(i)

[8] Similarly, confirmation of basic processes involved in monitoring Internet traffic—such as the creation of digital copies—would not reveal state secrets. These are processes the government has already disclosed, including in connection with NSA-assisted surveillance. *See, e.g.*, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion Detection System (EINSTEIN 2.0)*, 33 Op. O.L.C. 1, 4 (2009), https://perma.cc/8Z4Q-QM34; White House, *The Comprehensive National Cybersecurity Initiative*, https://perma.cc/R5TE-757K; DHS, *EINSTEIN 3 Privacy Impact Assessment* (Apr. 19, 2013), https://perma.cc/F665-Q5Z7.

concern electronic surveillance under FISA. *See* Def. Opp. 15–16.[9] Because these opinions do not address the central issue—*i.e.*, whether the specific discovery procedures in Section 1806(f) trump the more general language of Section 3024(i)—they provide no support for the government's assertion that Section 3024(i) controls here.

The government also asserts, incorrectly, that the information Wikimedia seeks is protected under 50 U.S.C. § 3605(a), a provision of the National Security Agency Act of 1959. *See* Def. Opp. 16–18. As with Section 3024(i), whatever the meaning of the general language of Section 3605(a), FISA's more specific and later-enacted discovery provision supersedes it in this case. *See, e.g.*, *Green*, 490 U.S. at 524–26; Pl. Br. 25–27.[10] Moreover, as Wikimedia explained in its opening brief, the government's strikingly broad interpretation of the scope of Section 3605(a) is belied by the legislative history and at odds with numerous provisions in FISA requiring NSA disclosures. *See* Pl. Br. 25–26; *see also, e.g.*, *Baldrige v. Shapiro*, 455 U.S. 345, 360 (1982) (statutes that create litigation privileges must be construed narrowly).

II. The NSA cannot withhold deposition testimony on the basis of the claimed privileges.

Wikimedia has moved to compel the NSA's Rule 30(b)(6) deposition testimony over numerous invocations of the state secrets privilege and other asserted privileges. Pl. Br. 10–11, 33. At the time Wikimedia filed its motion, the deposition had been noticed and the NSA had lodged objections, but the deposition had not yet taken place. The parties conducted the deposition on April 16, 2018. As anticipated, the NSA refused to respond to numerous questions

[9] *Linder v. Dep't of Defense*, 133 F.3d 17 (D.C. Cir. 1998) (wrongful death action); *Kronisch v. United States*, No. 93 CIV. 2458, 1995 WL 303625 (S.D.N.Y. May 18, 1995) (suit challenging CIA's human experimentation involving LSD); *United States v. Koreh*, 144 F.R.D. 218 (D.N.J. 1992) (denaturalization proceeding); *Heine v. Raus*, 261 F. Supp. 570 (D. Md. 1966) (defamation action); *CIA v. Sims*, 471 U.S. 159 (1985) (FOIA suit).

[10] Once again, none of the cases cited by the government in support of its argument concern electronic surveillance under FISA. *See* Def. Opp. 16–18.

on the basis of the state secrets privilege, Section 3024(i), and Section 3605(a). Importantly, the deposition questions go beyond the written discovery—for example, they ask the NSA to provide facts about Upstream surveillance where Defendants have said they will rely on the speculation of an outside expert. *See* Def. Mot. to Compel 10–11 (ECF No. 126-1). Defendants indicate that they will respond to any motion to compel deposition testimony at a later date, *see* Def. Opp. 7 n.5, but Wikimedia has already moved to compel that testimony in this motion, and both the Coats and Barnes Declarations address it, *see* Coats Decl. ¶¶ 9, 34, 48; Barnes Decl. ¶¶ 8, 9, 51–53, 56, 110, 118. Thus, the question of whether the NSA should be compelled to provide responses is ripe for resolution, and Wikimedia includes with this brief a list of questions the NSA refused to answer. Gorski Decl., Ex. 1.[11]

III. In camera review is practicable and would not result in an undue burden.

The government suggests that in camera review of its discovery responses would result in an intolerable burden. But the Court can structure its review to ensure manageability. Contrary to the government's claims, Wikimedia does not seek entire NSA databases, and the Court will not have to review tens of thousands of pages. *See* Def. Opp. 6, 33–34.

Defendants criticize Wikimedia for the number of its requests, but half of the requests at issue seek straightforward admissions—for instance, an admission that the NSA has reviewed

[11] Because it was unknown when the NSA would complete its classification review of the deposition transcript and release it to Wikimedia, Wikimedia originally proposed a procedure whereby, within two weeks of the Court's ruling on the question of whether Section 1806(f) controls, Wikimedia would supplement its motion to compel to individually list the questions the NSA should be required to answer. Pl. Br. 33–34. The deposition transcript is now available, however. Thus, in the interests of judicial economy, Wikimedia has included the list of questions here. Gorski Decl., Ex. 1. On April 18, 2018, Wikimedia filed a supplemental memorandum to more specifically identify its challenges to the NSA's refusal to respond to Wikimedia's deposition questions, including the NSA's objections that the questioning was outside the scope of the Rule 30(b)(6) notice, and that the NSA's witness was inadequately prepared to fully answer the questions posed. *See* Pl. Suppl. to Mot. to Compel (ECF No. 136). Should the Court desire additional briefing from the parties on those issues, Wikimedia will provide it.

the content of at least one Wikimedia communication (RFA No. 35), and that the NSA reviews the contents of Internet communications in bulk (RFA No. 8). *See* Toomey Decl., Ex. 1. The remaining requests seek information about the breadth of Upstream surveillance—such as the number of "international Internet link[s]" where Upstream surveillance occurs (in the FISC's words)—and the meaning of key terms the government itself has used in public documents. This information would aid an expert examining the scope and operation of Upstream surveillance as it bears on the interception of Wikimedia's communications.[12]

Defendants also make the eye-catching claim that responding to RFP Nos. 21 and 22 would require the Court to review 10,000 pages, but that is an exaggeration. *See* Def. Opp. 34. Inexplicably, the government ignores the fact that Wikimedia narrowed these two requests to focus on the most relevant categories of information, as set out in its motion to compel. *See* Toomey Decl., Ex. 1 at 15–16. Where possible, Wikimedia has already identified some of the most important of these documents for the Court, *see* Pl. Br. 9–10, but at present, only the government knows what is contained in the documents it is withholding in full.[13]

Moreover, the Court has the flexibility to structure its in camera review. It can enlist the parties' assistance in prioritizing certain information, including by ordering the government to produce relevant information in a clear and manageable form, as the district court ordered in *Jewel*. *See* Hr'g Tr. 70:22–74:10, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. May 19, 2017)

[12] Defendants' complaints about the amount of discovery ring hollow. In fact, the government demanded far more information from Wikimedia, serving dozens of multi-part interrogatories and requests for documents. The critical difference is that Wikimedia, where appropriate, provided meaningful responses and more than 9,000 pages of documents. Defendants, by contrast, only recapitulated information that was already publicly available.

[13] Defendants notably omit Wikimedia's repeated efforts to narrow these requests through the parties' negotiations. On February 6, 2018, and March 13, 2018, Wikimedia provided Defendants with lists of search terms that would help identify the most relevant documents. The government first said it would not conduct such a search; then, the night before fact discovery closed, the government informed Wikimedia that time to conduct a search had run out.

(ECF No. 362) (setting terms for the government's production of evidence for in camera review). It can also require Defendants to affirm or deny straightforward facts about the surveillance of Wikimedia, and it can rely on the assistance and expertise of a special master to review information about the breadth of Upstream surveillance.

Although Defendants paint Wikimedia's motion as a radical one, Wikimedia is simply asking the Court to review the same kind of information that the government routinely provides to district courts and the FISC when they review these same activities in other types of proceedings pursuant to FISA. Indeed, the government has *already* disclosed a significant share of the information at issue to other courts for in camera and ex parte review.

IV. Defendants' other objections are groundless.

A. Wikimedia's discovery requests are relevant to jurisdiction.

Defendants wrongly argue that several categories of information have "no bearing" on the question of jurisdiction. Def. Opp. 32–33. First, the definitions of terms that the government has used to describe Upstream surveillance are crucial to understanding how it operates from a technical perspective. Second, the volume of communications processed and retained in the course of Upstream surveillance bears directly on the scope of this surveillance. Third, the targeting procedures are relevant because they discuss the international Internet links at which Upstream surveillance takes place. *See* 2009 NSA Targeting Procedures at 2 (Toomey Decl., Ex. 2 at 29, ECF No. 125-5). Finally, the fact that some documents Wikimedia sought to authenticate do not, "on their face," make explicit references to "Upstream," the "NSA," or "Wikimedia," Def. Opp. 33, does not render them irrelevant. A document can contain relevant information without stating the names of the parties. *See* Fed. R. Evid. 401. At bottom, Defendants' arguments are at odds with common sense and the liberal discovery standards in the Federal

Rules of Civil Procedure.[14]

B. Wikimedia's RFAs are proper and Defendants must answer them.

Defendants contend that RFAs are not meant to be used as "general discovery devices" on matters for which the requesting party has no "sources of competent proof." Def. Opp. 35. Defendants cite no authority in the Fourth Circuit supporting that proposition, and Wikimedia's RFAs are entirely proper. *See, e.g.*, *House v. Giant of Md., LLC*, 232 F.R.D. 257, 262 (E.D. Va. 2005).[15] If, for example, Defendants admitted that the NSA reviews the contents of Internet communications, *see* RFA No. 6 (Toomey Decl., Ex. 1), or that it conducts Upstream surveillance on Internet circuits, *see* RFA No. 13, the range of genuine issues for determination during this jurisdictional phase would be narrowed—the very purpose of RFAs.

Instead, by recasting Wikimedia's requests in their own words, Defendants have chosen to neither admit nor deny Wikimedia's requests. This gamesmanship is improper. *See Poole ex rel. Elliott v. Textron, Inc.*, 192 F.R.D. 494, 499 (D. Md. 2000). Defendants should be ordered to answer Wikimedia's requests, or the requests should be deemed admitted. *See* Fed. R. Civ. P. 36(a)(6) ("Unless the court finds an objection justified, it must order that an answer be served.").

Conclusion

For the foregoing reasons, Plaintiff's motion to compel should be granted.

---

[14] *See* Fed. R. Civ. P. 26(b)(1); *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978); *Santos v. Crowell*, No. 15-3907, 2016 WL 6068082, at *4 (D. Md. Oct. 17, 2016).

[15] None of the cases Defendants cite uphold an objection to RFAs because the requests were improperly used as "general discovery devices," or because the requesting party lacked "sources of competent proof." In *Graphic Sec. Sys. Corp. v. Nautilus Sec.*, No. 08-4034, 2010 WL 11534374, at *2 (D.S.C. Aug. 20, 2010), the court refused to compel RFA responses, stating in dictum that the requests for admission did "not elicit new evidence," because—unlike here—the requesting party served an additional fifty requests ten months into the discovery period.

Dated: May 18, 2018

Respectfully submitted,

/s/
Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Road, #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

Benjamin H. Kleine (pro hac vice)
Devon Hanley Cook (pro hac vice)
Molly A. Smolen (pro hac vice)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

/s/
Ashley Gorski (pro hac vice)
(*signed by Ashley Gorski with permission of Deborah A. Jeon*)
Patrick Toomey (pro hac vice)
Jonathan Hafetz (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff